Requested Patent: WO0070456A1

Title:

A DISTRIBUTED SYSTEM AND METHOD FOR SYSTEM IDENTIFICATION AND VULNERABILITY SCANNING ;

Abstracted Patent: WO0070456 ;

Publication Date: 2000-11-23 ;

Inventor(s): BEEBE TODD (US); HEILMANN CRAIG (US) ;

Applicant(s):

BEEBE TODD (US); HEILMANN CRAIG (US); SECURELOGIX CORP (US) ;

Application Number: WO1999US22240 19990924 ;

Priority Number(s): US19990312365 19990514 ;

IPC Classification: G06F11/00; G06F11/34; H04K1/00 ;

Equivalents: AU6264799 ;

ABSTRACT:

A system and method for a distributed system for identification of network access points into a secure network. The system and method include: a means for dialing a plurality of telephone numbers (310, 308, 306) and logging results for each telephone number; a means for remotely managing the means for dialing (312, 314), and a means for reporting the results for each telephone number (422). The system may also include a means (300, 302, 304) for identification of the network access points by detecting Point to Point Protocol (PPP) and password guessing in an attempt to gain access to the communications resource. The system can also include a means for identification of the network access points by detecting binary and/or text signatures. The system can also include a means (310, 308, 306) for dialing at least two telephone numbers at the same time. The system can also include remotely dialing local telephone numbers. The system can also include reporting changes in dialup access points since a previous scan.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 11/00, 11/34, H04K 1/00

A1

(11) International Publication Number: WO 00/70456

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US99/22240

(22) International Filing Date: 24 September 1999 (24.09.99)

(30) Priority Data:
09/312,365 14 May 1999 (14.05.99) US

(71) Applicant *(for all designated States except US)*: SECUREL-OGIX CORPORATION [US/US]; Suite 230, 13750 San Pedro, San Antonio, TX 78232 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BEEBE, Todd [US/US]; 2806 Enchanted Landing Court, Katy, TX 77494 (US). HEILMANN, Craig [US/US]; 7910 Las Olas Boulevard, San Antonio, TX 78250 (US).

(74) Agents: McCOMBS, David, L. et al.; Haynes and Boone, L.L.P., Suite 3100, 901 Main Street, Dallas, TX 75202-3789 (US).

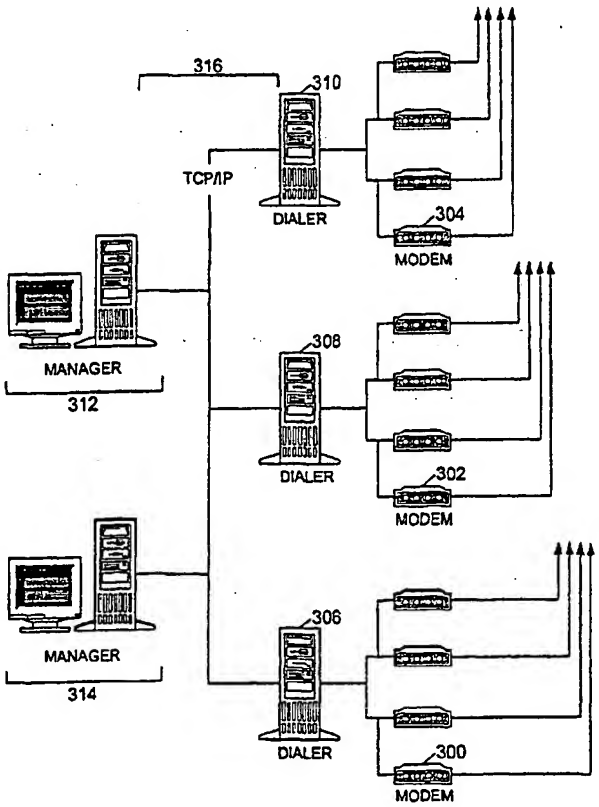
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A DISTRIBUTED SYSTEM AND METHOD FOR SYSTEM IDENTIFICATION AND VULNERABILITY SCANNING

(57) Abstract

A system and method for a distributed system for identification of network access points into a secure network. The system and method include: a means for dialing a plurality of telephone numbers (310, 308, 306) and logging results for each telephone number; a means for remotely managing the means for dialing (312, 314), and a means for reporting the results for each telephone number (422). The system may also include a means (300, 302, 304) for identification of the network access points by detecting Point to Point Protocol (PPP) and password guessing in an attempt to gain access to the communications resource. The system can also include a means for identification of the network access points by detecting binary and/or text signatures. The system can also include a means (310, 308, 306) for dialing at least two telephone numbers at the same time. The system can also include remotely dialing local telephone numbers. The system can also include reporting changes in dialup access points since a previous scan.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A DISTRIBUTED SYSTEM AND METHOD FOR SYSTEM IDENTIFICATION AND VULNERABILITY SCANNING

TECHNICAL FIELD

The invention relates generally to telecommunications access control systems and particularly to a telephony system for identifying systems and vulnerability scanning for secure networks.

BACKGROUND

Firewalls have proven effective in protecting the perimeter of computer data networks and are now considered to be essential network components. However, firewalls and intrusion detection devices provide no protection against unauthorized traffic routed to or from the network through devices such as modems.

Most organizations protect authorized modem access to their computer networks with authentication and encryption technologies, bundled into Remote Access Services (RAS). However, organizations recognize the very real and growing threat posed by unauthorized access to the network through rogue modems, easily connected to nearly any of its voice or fax lines. Security savvy organizations are becoming increasingly effective in protecting computer access to their networks; and at the same time, acutely aware of the threats posed by lack of security over access to the same networks through their hundreds or even thousands of uncontrolled, unmonitored telephone lines.

Modems and fax machines connected to an organization's data network can be installed by individuals with either malicious or benign intentions. Nearly any individual can easily connect a modem to an existing PC and/or telephone or facsimile line. Once connected, the device effectively bridges the "untrusted" Public Switched Telephone Network (PSTN) to an organization's "trusted" data network. Each bridge can be thought of as an unmonitored, uncontrolled connection to the Internet, or "untrusted" network. An individual with benign intentions might utilize this access to the data network to unknowingly upload data containing dangerous viruses, bypassing the protection and logging provided by a firewall. More importantly, individuals having malicious intent can exploit this same bridge to the "trusted" data network. Hackers and phreakers will often wardial to

find these bridges, then gain access to the data network potentially stealing and/or destroying valuable data behind the front line protection of the firewall.

Interestingly, the same tools that are used to exploit security are also used routinely by security professionals to help secure their private data networks by locating, identifying and testing the security configuration of modems providing access to the network.

Though a handful of commercially produced wardialers have emerged over the past several years, the basic theme of operation has not changed for more than twenty years. Wardialers remain standalone applications, dialing ranges of numbers, identifying those with carriers, and in some more sophisticated cases, attempting to identify the communications software at the other end; for instance, PC Anywhere, NT RAS, or simply a VT100 emulated shell.

The fact that a large portion of an organization's data network goes unprotected has not completely escaped the attention of savvy security Managers. This is especially significant when you consider the sheer number of telecommunication "pipes" that are connected to an organization's network. The extraordinarily low cost and knowledge barrier associated with modem technology today exacerbates the problem of unsecured modems discussed above. Almost anyone can simply connect a modem to a PC on the trusted data network, effectively bridging the trusted network to the untrusted PSTN. Periodic scanning of the telephone network is now generally recognized as a necessary component of a corporate security policy. In fact, a significant number of organizations have begun using a variety of ad-hoc tools to survey their telecommunication security posture.

Currently, the data security market is focused primarily on LAN, WAN, and Internet security. Traditional firewalls generally protect TCP/IP-based networks (or other packet-based protocol networks), attempting to restrict access and to protect data on networks behind them. Most, however, are focused on protecting the "front-door" (the Internet) while ignoring the "back door, side door and windows" (the telecommunications access to the data network).

Initially, the only tools available to security professionals were wardialers that were originally developed by underground "hackers" and telephone "phreakers." There are a number of problems associated with the use of a product developed and intended largely for

malicious purposes. The primary problem is that the software was not developed and tested using acceptable levels of engineering discipline. Furthermore, those types of applications may even contain undocumented features, Trojan Horses or computer viruses. For a long time, there were no companies in the industry producing commercially developed wardialers. Security professionals were forced to rely on untested and unproven tools because they often were not in a position to develop the tools themselves or contract another company to develop the tools professionally. This unfulfilled need spurned the development of security-centric and professionally developed telephone scanning products.

Today, many wardialers are available to security professionals. Most of these software applications vary in complexity and were developed by individuals in the hacker community. Some available wardialers operate using a single computer and a single modem, while others can control multiple modems simultaneously. The primary benefit of this multiple modem control feature to the security professional is the decrease in time required to complete a sweep of several hundred or more telephone lines. Although able to dial multiple modems simultaneously, multiple modem systems are not cost effective when used on a large, geographically separated organization due to the cost of extended long distance dialing required to accomplish a complete scan of the enterprise. Additionally, since existing systems do not provide a distributed solution, the results from multiple, independent scans from geographically separate sites must be manually analyzed and compared to ascertain the complete corporate security posture.

Therefore, a dependable, user friendly, scalable, and reliable system and method for identifying systems and vulnerability scanning for secure networks is needed to fill these needs.

SUMMARY OF THE INVENTION

The present invention is a software application and architecture that expands traditional wardialing functionality to include system identification and vulnerability scanning, while providing large scale distributed and parallel execution through a client-server architecture. In this fashion, an organization can reduce costs and effectively leverage security expertise across their enterprise. Currently, security professionals have a limited set of reliable, professionally developed scanning products to use to characterize their

telecommunications security posture. A pressing need exists to develop a commercial grade wardialer with enhanced functionality.

The present invention is a telecommunications scanner, which performs advanced dialing and vulnerability assessment functions for telephonic networks. The present invention provides an important fundamental benefit in that it provides visibility into the existence of rogue modems and characterization of the security risks they impose. By logging the vulnerability state of modems connected to the trusted data network, the scanner provides visibility into the usage of telecommunications resources, thereby enhancing an organization's ability to more completely assess their security posture. This enables the organization's decision-makers to evaluate, monitor and improve security policies, which include telecommunication resources. In addition to the visibility provided by logging communication events, the present invention is capable of automatically detecting and identifying the software controlling the modem, and testing its configuration to determine its security posture. The visibility provided goes beyond merely logging the existence of modems connecting the PSTN to the trusted data network. The scanning system is capable of detecting changes in the number and security state of modems that have occurred since the last "sweep". The present invention detects, analyzes and reports the potential vulnerability of each and every telephone station, fax machine, and modem line in the enterprise at a discrete point in time. Use of its "compare" feature allows security professionals to compare the results from several discrete assessments, to detect and analyze vulnerability trends.

The present invention is a client/server solution for telecommunication vulnerability assessment. In this design, the server is the Manager and the client is the Dialer. The Manager is used to configure the rule set for dialing and then receive, display and interpret the results. The Manager develops dialing profiles and then pushes those profiles to Dialers for execution. Each Dialer operates one or more modems to perform each dialing task as defined by the Manager. It categorizes each phone line dialed as voice, fax or modem and marks uncompleted calls such as busy or no answer to be called again in accordance with the dialing policy.

For large organizations, which may be geographically separated, the present

invention can consist of multiple Dialers and Managers, interconnected by a LAN/WAN or the Internet itself, thus providing remote, centrally managed enterprise-wide characterization of the organization's telephony security posture.

In one embodiment, a system and method for a distributed system for identification of network access points into a secure network is provided.. The system and method includes: a means for dialing a plurality of telephone numbers and logging results for each telephone number; a means for remotely managing the means for dialing; and a means for reporting the results for each telephone number. The system may also include a means for identification of the network access points by detecting Point to Point Protocol (PPP) and password guessing in an attempt to gain access to the communications resource. The system can also include a means for identification of the network access points by detecting binary and/or text signatures. The system can also include a means for dialing at least two telephone numbers at the same time. The system can also include remotely dialing local telephone numbers. The system can also include reporting changes in dialup access points since a previous scan.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a functional block diagram of an exemplary communications network;

FIG. 2 is an architectural diagram of the preferred embodiment of the present invention showing a standalone configuration;

FIG. 3 is an architectural diagram of the preferred embodiment of the present invention showing a distributed configuration;

FIG. 4 is a flow diagram illustrating the Manager portion of the system;

FIG. 5 is a flow diagram illustrating the Dialer control interface portion of the system; and

FIG. 6 is a flow diagram illustrating the Dialer portion of the system.

DETAILED DESCRIPTION

One of the first steps in securing an organization is locating all access points, determining how secure those access points are, then locking them down. Insecure or misconfigured modems with an organization are security risks, potentially bypassing controls normally enforced by firewalls or similar security devices. Security personnel must

be able to detect all modems and faxes first, and then make an additional determination as to which ones are authorized and which ones are not. Once identified, security personnel can eliminate the unauthorized modems and manage the security configuration of the authorized modems. The preferred embodiment performs the identification piece by scanning the network for modems connected to the network, followed up with an assessment of each modem's security posture.

In figure 1, an attacker 100 can access a communications network by either going through the Internet 102 or the Public Switched Telephone Network (PSTN) 104. The Internet 102 connects to the internal network 106 through a router 108 and a firewall 110. The router 108 routes all traffic into the internal network 106 from the Internet 102, as well as all traffic out to Internet 102. However, the firewall 110 has the power to restrict all traffic going in and out of the internal network 106.

Although the internal network 106 depicted in figure 1 has a firewall 110 to prevent unauthorized traffic, the attacker has another access point through the PSTN 104. A Remote Access Server (RAS) 120 connects a Private Branch eXchange (PBX) 114 to the internal network 106, but through the firewall 110. This configuration allows users remote access to the internal network, but does so securely since the user must go through the firewall 110. However, as depicted in figure 1, a user may have a modem 112 connected to his computer 122 and allow access into the internal network 106. In this scenario, the attacker 100 can use a wardialer to find the modem 112 connected to the internal network 106 and then attempt to gain access through the modem 112. The wardialer could also detect a telephone 116 and a fax machine 118, but is mainly interested in the modem 112.

The scenario depicted in figure 1 shows how the security of an internal network can be threatened even though a firewall is installed to protect the network.

Figure 2 shows the architecture of the standalone configuration of the present invention. The system consists of several modems 200 that dial phone numbers in order to detect other modems connected to a network. The modems 200 are controlled by a software program called a Dialer. The Dialer is described in more detail below in reference to figures 5 and 6. In the standalone configuration of figure 2, a Dialer is run on a single computer along with the Manager portion of the present invention. The Manager portion is described

in detail below in reference to figure 4.

The present invention includes dialing ranges of numbers, identifying modem and/or fax carriers, and attempting to identify the communications application at the terminating station through signature analysis (i.e. matching negotiation signaling and/or textual "banners" to known system types).

After identifying the communications application at the terminating station, the present invention attempts to establish a connection and test for security vulnerabilities associated with it. For example, if the present invention determines it has dialed into a modem on a PC that is running PCAnywhere, it will attempt to gain access to the PC using default PC Anywhere UserID and Password combinations. Most wardialing applications do not offer this level of assessment. The object of this extended capability is to confirm potential vulnerabilities and characterize the level of security of telephony devices (primarily modems) in the same manner that TCP/IP security scanners test for and characterize the security posture of network devices.

Due to their distributed nature, many organizations need to define, determine, characterize and enforce telecommunications security policy across the enterprise. The preferred embodiment includes the ability to remotely manage administration, configuration and service. Additionally, the present invention enables a large-scale organization to limit duplication of effort and ensure consistent application of security policy across a distributed organization. Although security systems are necessarily distributed, policy is usually dictated centrally. This requires an organization to control security devices in a top-down fashion. In order to assess the enterprise-wide security posture, detailed visibility into the entire organizational data stream is necessary. This detailed visibility is provided by collection at the device level, reporting up the management chain, and consolidating multiple reports at the Manager.

The system architecture depicted in figure 3 supports distribution of the dialing software to remote locations, controlled and managed via TCP/IP 316 connections (e.g., over internal LANs, private WANs, or even over the Internet). To make the system as flexible as possible, one or more management GUIs are located on computers 312 and 314 and control one or more Dialers 306, 308 and 310 whether collocated on a single platform, or distributed

around the globe via the Internet. Each Dialer 306, 308, and 310 has a set of modems 300, 302, and 304 respectively, that can operate in parallel. With this type of configuration, geographically separated organizations can leverage local dialing resources, executing very large scale scans in parallel, then consolidating the results on-screen and in reports at a single location. The advantages are fast, extensive parallel execution and low cost since most, or all, calls are local in nature as opposed to the substantial cost of dialing long distance. In many cases, dialing can be accomplished entirely through local PBXs without ever passing to the local carrier; an additional cost consideration when local calls are billed, as is the case in most European countries. In addition, although two Managers are shown, one Manager could also be configured to control all of the Dialers.

By operating in parallel, the present invention can accomplish very large scale scans in minimum time. A typical wardialer will get through 100 numbers per hour, per modem it uses. In addition, most wardialers use only one modem. The present invention can use as many modems as the operating system will allow, and coordinates the scan among all the Dialers. In a scenario of a widely dispersed global company owning 3 million numbers, it would take a typical wardialer about 30,000 hours. When the present invention is configured with 50 Dialers with 2 modems each, the scan would only take 300 hours to complete. A system configured as depicted in figure 3 with 3 Dialers 306, 308, and 310 with 4 modems 300, 302, and 304 each, the scan would take 2500 hours, which is still a considerable savings on time over the typical wardialer.

The Managers also control logging the results of the Managers and the Dialers. The logs include system service/performance as well as the dialing results. Specifically, the log files contain entries of all event messages. Configuration settings determine the level of logging for both service/performance and dialing results. In the distributed architecture, the centrally controlled Manager pushes the configuration down to one or more of the remote dialing applications. The reporting aspect also has the capability to report only "deltas" or changes from one scan to the next. This allows security personnel to execute monthly or bi-weekly scans and find out only what's changed since the last scan.

Figure 4 shows details of how the Manager functions and interacts with the Dialers. First, the Manager is installed and configured in module 400. The Manager then configures

the profiles and the Dialers in module 402. The levels of logging performed by the Dialers are configurable (i.e. informational, warning, critical, etc.) by the user. The Manager then sends sweep information to the Dialers in module 404. When the Managers task Dialers to perform dialing jobs, each job is traceable to the Manager that assigned that particular job. A decision is then made on whether to shutdown in module 406. If the shutdown instruction is entered, the Manager then restarts in module 510. If the Manager is not to shutdown, the program then views the live results represented by module 408. Logs generated by Dialers are available for display in real time while dialing tasks are underway. Once the user finishes viewing the live results, the Manager returns to the user options in module 416.

Once the Manager is restarted, it then connects to known Dialers in module 412 and retrieves results in module 414. The Manager then gives the user three options in module 416. One of the options is to send sweep information represented by module 418. Another option is to view or compare the results represented by module 420. When the dialing jobs are complete, the Manager consolidates results from all participating Dialers into a single report. A third option is to configure profiles and/or the Dialers represented by module 422.

The present invention also includes system service/performance logs. Logging system service/performance is a common feature of high-reliability products. It involves logging service events and performance of hardware and software components to simplify troubleshooting and provide decision support.

The present invention includes a dialing results log. Logging dialing results involves recording communications details for real-time display and post-activity analysis. Details recorded include, but are not limited to:

- Job Number
- Destination phone number
- Call type (voice, modem, fax)
- Job start date-time group
- Job end date-time group
- Job duration
- Action(s) performed
- If modem or fax is detected:

- Name & type of application detected
- Type of vulnerability assessment performed, if any (Password guess, etc.)
- Result of vulnerability assessment
- Record the printing and non-printing characters in the banner

In order to assess organizational security posture, detailed visibility into the corporate data stream is necessary. This detailed visibility is provided by collection at the device level, reporting up the management chain, and consolidating multiple reports at the Manager. The present invention is capable of generating reports based on the results of its security sweeps on demand. Data reduction and collation is also supported to aid the security staff in their analysis of the current security posture and in detecting and characterizing trends in telecommunications security. Since the present invention can be configured to be either a standalone (Manager and Dialer on same platform), or as distributed system (Manager and Dialers on separate platforms), it also supports the capability for local report generation based only on the data gathered locally. The Manager also accepts, collates and sorts reports from multiple Dialers to aid in analysis of the enterprise-wide security posture.

Security personnel require more than just a "snap shot" of the organization's current security posture. Running several sweeps and then manually collating the vast amount of information to look for trends, is time consuming, difficult and prone to human error. The preferred embodiment automatically collates the results from a series of sweeps over a period of time to be able to identify and analyze security trends. The results of trend analysis are then used to improve or reinforce organizational security policy. For instance, a lax security awareness environment in one department may manifest itself in a string of unauthorized modem detection events over a period of several months. This may necessitate further education or corrective action by the security staff.

Now turning to figure 5, more details of the Dialers will be described. The Dialer starts with and installation and configuration represented by module 500. The Dialer then starts the Dialer process in module 502. The Dialer then has to accept a connection from the Manager in module 504. In the preferred embodiment, the Dialer then exchanges licensing information with the Manager in module 506. A variety of licensing schemes may be used in

order to ensure that the Manages and Dialers are properly licensed. In addition, since the Dialers and Managers may be remotely connected through the Internet, they may use encryption in order to secure communications. If so, a variety of encryption schemes can be used. The Dialer then receives commands from the Manager in module 508, and then determined whether there are results to send in module 510. If there are no results to send, the Dialer then returns to module 504 to accept Manager connections. If there are any results to send to the Manager, the Dialer then determines if there is a connection to send the results to in module 512. If not, the Dialer again returns back to module 504. If a connection exists, then the Dialer sends the results to the appropriate Manager in module 514.

Now turning to Figure 6, more details of the Dialer's functions will be described. The Dialer first determines if there are any numbers to dial in module 600. From a logical flow perspective, the dialer remains in an active dialing loop until all numbers assigned to a particular profile have been dialed. At the start of the loop, the Dialer determines if there are more numbers left to dial, if so, it dials the next telephone number in the queue, represented by module 602. If the Dialer receives a connection in module 604, the Dialer then tries to detect what type of system it is in module 606. If the Dialer determines the connected system is a known system in module 608, the Dialer then attempts to penetrate the known system in module 610. The Dialer will log activity associated with each number, whether or not the Dialer was able to identify or penetrate the system at the receiving end.

Although illustrative embodiments of the invention have been shown and described, a wide range of modification, change and substitution is intended in the foregoing disclosure and in some instances some features of the present invention may be employed without a corresponding use of the other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

WHAT IS CLAIMED IS:

1. A distributed system for identification of dialup access points into computer networks, the system comprises:

means for dialing a plurality of telephone numbers and logging results for each telephone number;

means for remotely managing the means for dialing; and

means for reporting the results for each telephone number.

2. The system of claim 1 further including means for identification of the network access points by detecting Point to Point Protocol (PPP) and password guessing in an attempt to gain access to the communications resource.

3. The system of claim 1 further including means for identification of the network access points by detecting binary and/or text signatures.

4. The system of claim 1 wherein the means for remotely managing the means for dialing includes managing at least two means for dialing at the same time.

5. The system of claim 4 wherein the at least two means for dialing includes at least two modems in each means for dialing.

6. The system of claim 1 wherein the means for dialing a plurality of telephone numbers include dialing only local telephone numbers.

7. The system of claim 1 wherein the means for reporting includes means for reporting changes in dialup access points since a previous scan.

8. A method for identifying dialup access points into computer networks, the method comprises:

dialing a plurality of telephone numbers and logging results for each telephone

number;

remotely managing the dialing; and

reporting the results for each telephone number.

9. The method of claim 8 further including detecting Point to Point Protocol (PPP) and password guessing in an attempt to gain access to the communications resource.

10. The method of claim 8 further including detecting binary and/or text signatures.

11. The method of claim 8 wherein the remotely managing includes dialing at least two telephone numbers at the same time.

12. The method of claim 11 wherein the dialing the at least two telephone numbers includes dialing from at least two modems on one Dialer.

13. The method of claim 8 wherein the dialing of a plurality of telephone numbers include dialing only local telephone numbers.

14. The system of claim 8 wherein the reporting includes reporting changes in dialup access points since a previous scan.

15. A computer software system for identifying dialup access points into computer networks, the system comprises:

computer instructions for dialing a plurality of telephone numbers and logging results for each telephone number;

computer instructions for remotely managing the dialing; and

computer instructions for reporting the results for each telephone number.

16. The system of claim 15 further including computer instructions for detecting Point to Point Protocol (PPP) and password guessing in an attempt to gain access to the communications resource.

17. The system of claim 15 further including computer instructions for detecting binary and/or text signatures.

18. The system of claim 15 wherein the computer instructions for remotely managing includes computer instructions for dialing at least two telephone numbers at the same time.

19. The system of claim 18 wherein the computer instructions for dialing the at least two telephone numbers includes computer instructions for dialing for at least two modems on one Dialer.

20. The system of claim 15 wherein the computer instructions for dialing a plurality of telephone numbers include computer instructions for dialing only local telephone numbers.

21. The system of claim 15 wherein the computer instructions for reporting includes computer instructions for reporting changes in dialup access points since a previous scan.

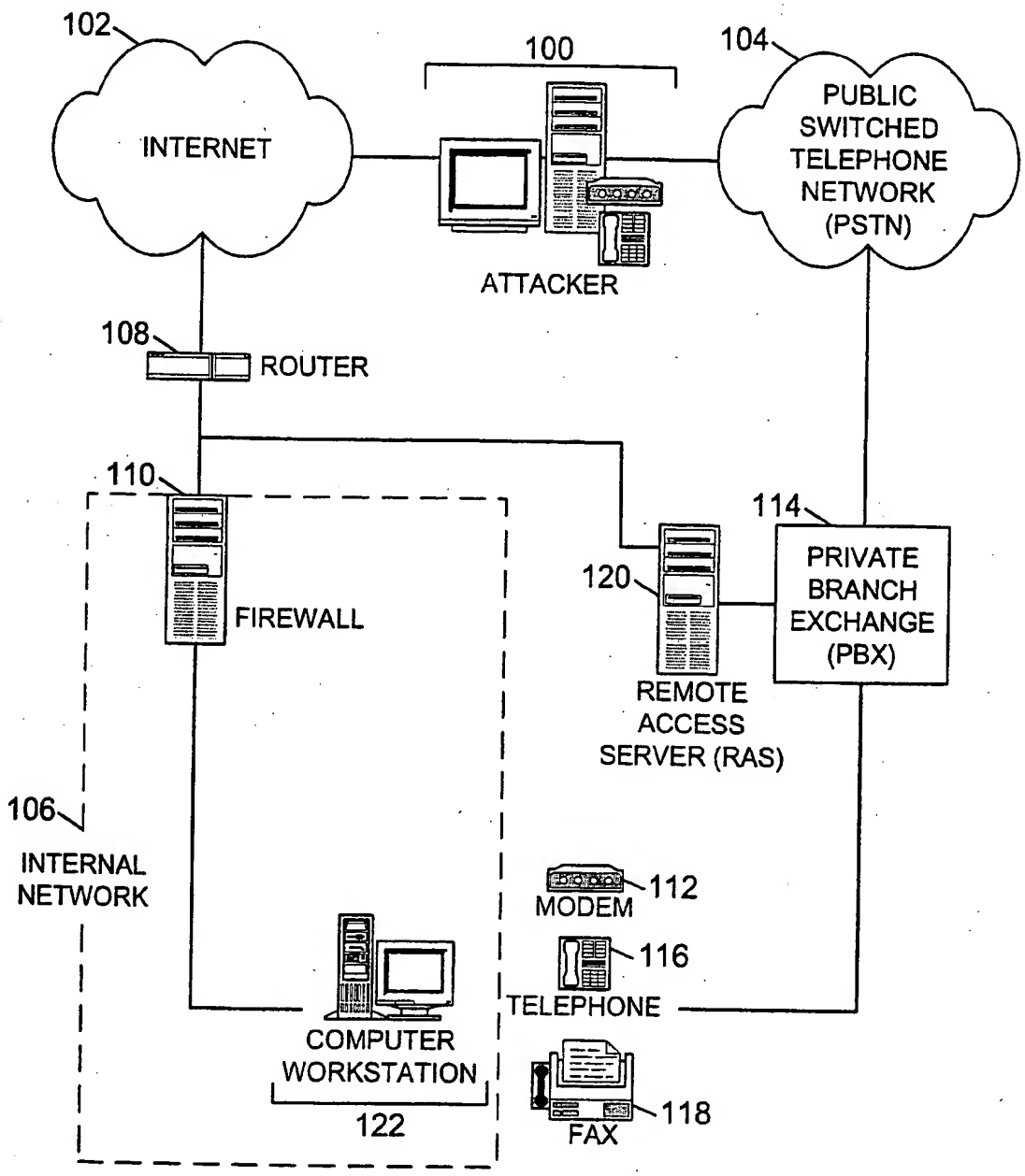

102
INTERNET
100
ATTACKER
104
PUBLIC SWITCHED TELEPHONE NETWORK (PSTN)
108
ROUTER
110
FIREWALL
120
REMOTE ACCESS SERVER (RAS)
114
PRIVATE BRANCH EXCHANGE (PBX)
106
INTERNAL NETWORK
MODEM
112
116
TELEPHONE
COMPUTER WORKSTATION
122
FAX
118

FIG. 1

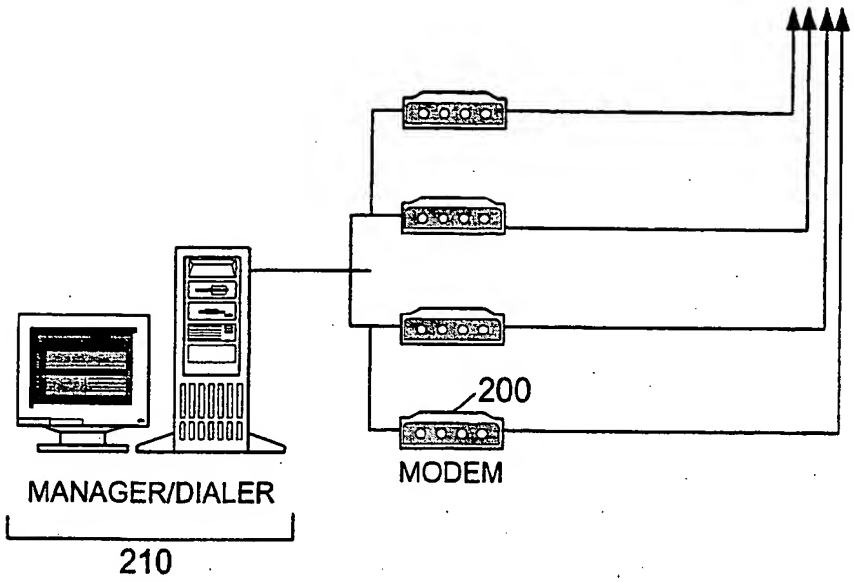


FIG. 2

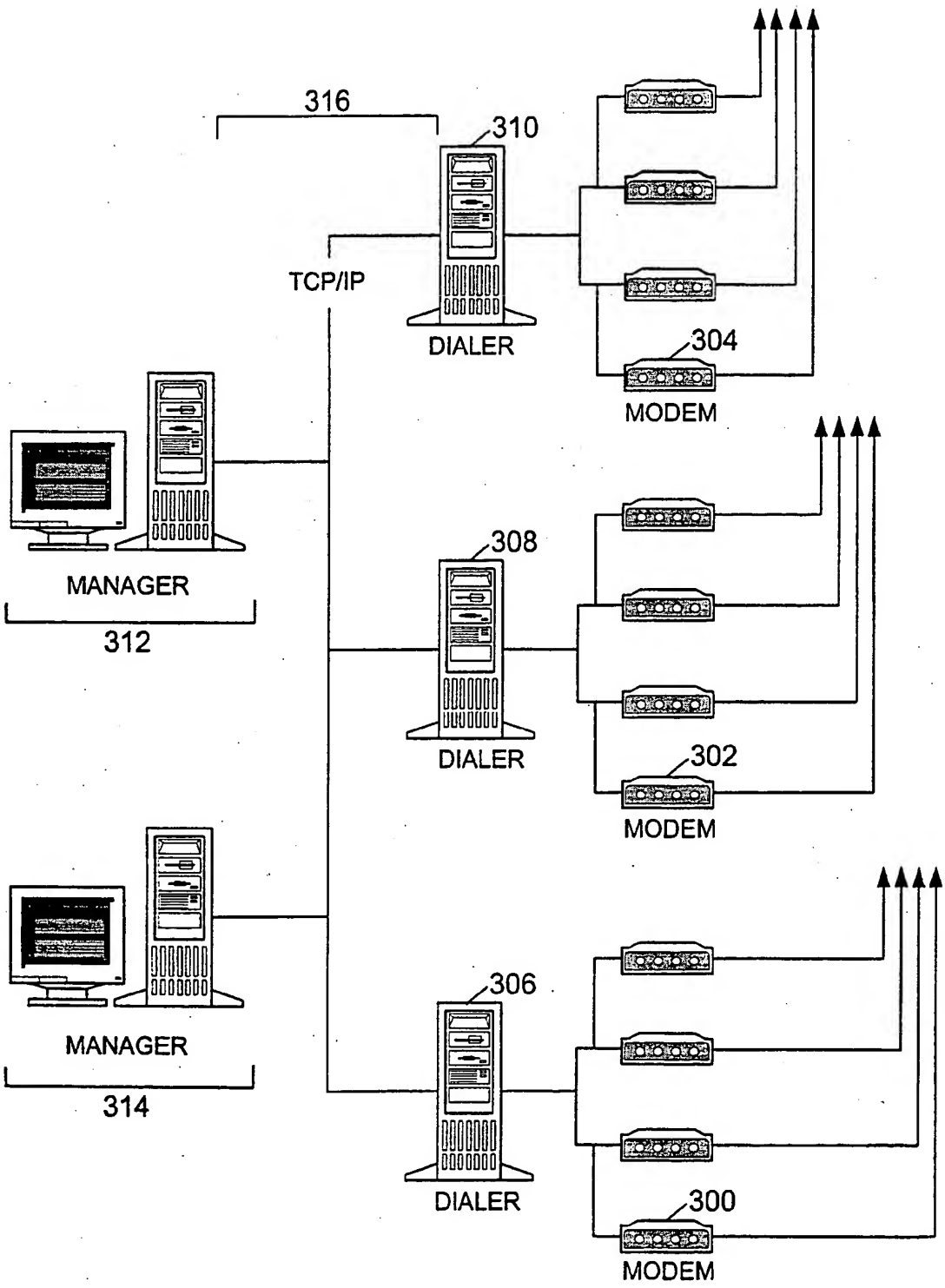

316
310
TCP/IP
DIALER
304
MODEM
MANAGER
312
308
DIALER
302
MODEM
MANAGER
314
306
DIALER
300
MODEM

FIG. 3

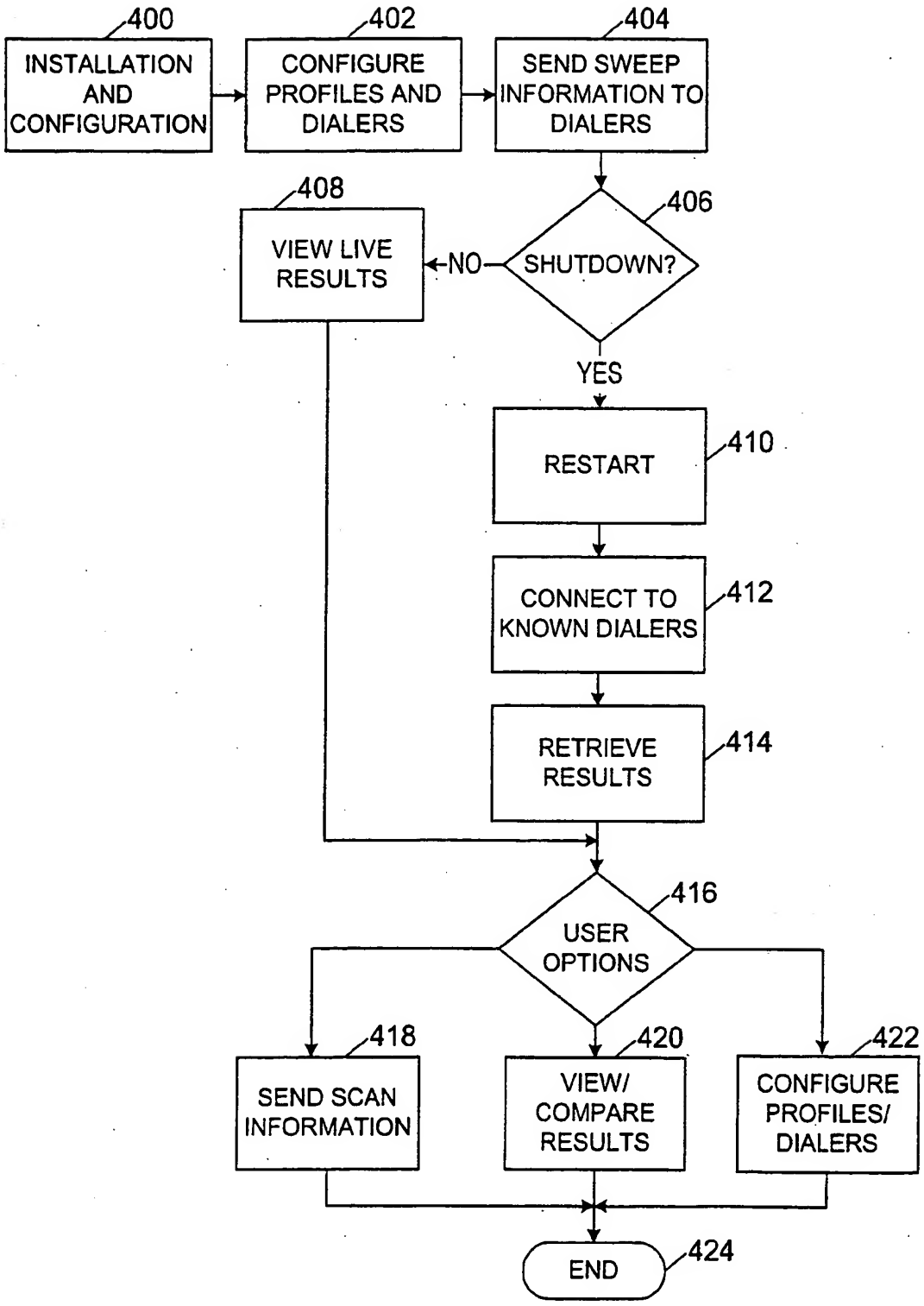

400
INSTALLATION AND CONFIGURATION
402
CONFIGURE PROFILES AND DIALERS
404
SEND SWEEP INFORMATION TO DIALERS
406
SHUTDOWN?
NO
408
VIEW LIVE RESULTS
YES
410
RESTART
412
CONNECT TO KNOWN DIALERS
414
RETRIEVE RESULTS
416
USER OPTIONS
418
SEND SCAN INFORMATION
420
VIEW/ COMPARE RESULTS
422
CONFIGURE PROFILES/ DIALERS
424
END

FIG. 4

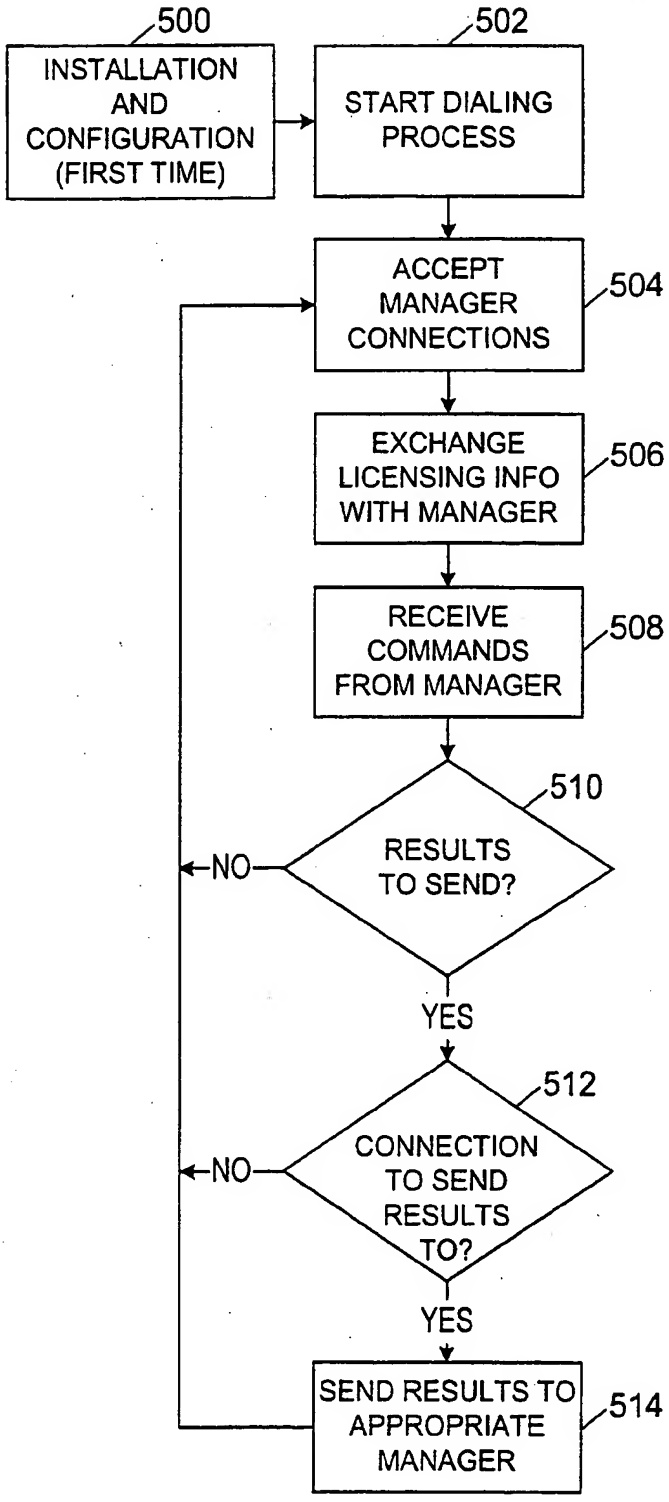

500
INSTALLATION AND CONFIGURATION (FIRST TIME)
502
START DIALING PROCESS
ACCEPT MANAGER CONNECTIONS
504
EXCHANGE LICENSING INFO WITH MANAGER
506
RECEIVE COMMANDS FROM MANAGER
508
510
RESULTS TO SEND?
NO
YES
512
CONNECTION TO SEND RESULTS TO?
NO
YES
SEND RESULTS TO APPROPRIATE MANAGER
514

FIG. 5

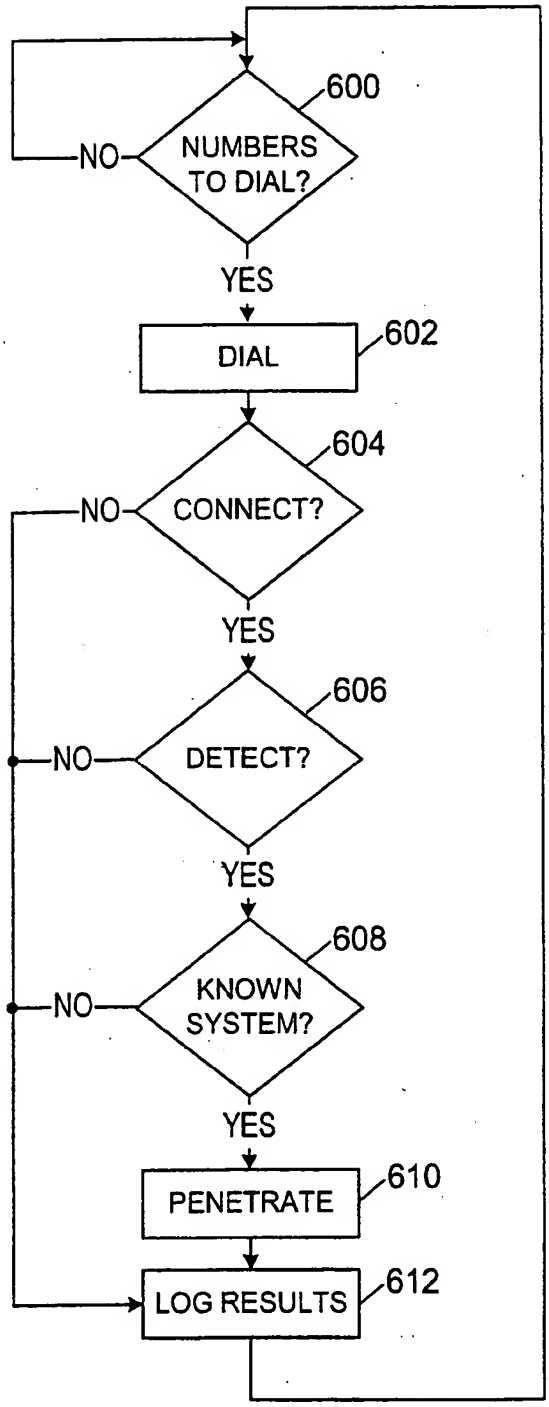

600
NUMBERS TO DIAL?
NO
YES
602
DIAL
604
CONNECT?
NO
YES
606
DETECT?
NO
YES
608
KNOWN SYSTEM?
NO
YES
610
PENETRATE
612
LOG RESULTS

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/22240

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G 06F 11/00, 11/34; H04K 1/00
US CL : 709/227; 370/400, 403; 713/200, 201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S : 709/227; 370/400, 403; 713/200, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,892,903 A (KLAUS et al) 06 April 1999, abstract, col. 6, lines 22-68-col. 7, lines 1-60.	1-21
Y	US 5,311,593 A (CARMI) 10 May 1994, col. 1, line 62- col. 3, line 65.	1-21
Y	US 5,557,742 A (SMAHA et al) 17 September 1996, col. 4, line 35-col. 14, line 27.	1-21
Y	US 5,623,601 A (VU) 22 April 1997, col. 7, line 20-col. 14, line 3.	1-21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 DECEMBER 1999	Date of mailing of the international search report 10 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer HIEU C. LE Telephone No. (703) 306-3101